McAfee®

Statement of SCAP Compliance

Statement of SCAP Implementation

McAfee Vulnerability Manager (formerly Foundstone Enterprise) provides a number of SCAP defined capabilities in an enterprise setting:

- Federal Desktop Core Configuration (FDCC) Scanner
- Authenticated Configuration Scanner
- Authenticated Vulnerability and Patch Scanner
- Unauthenticated Vulnerability Scanner
- And more.

McAfee Vulnerability Manager quickly discovers and identifies assets on a network using a highly parallel, patented technique capable of regularly scanning entire class-B networks from a single scan engine.

The product can then assess each detected system for open vulnerabilities, information leakages, misconfigurations, security holes, policy compliance, and more, using proprietary content professionally developed by McAfee Avert® Labs. Many of these checks can optionally be run "intrusively" to prove existence of vulnerabilities by actually exploiting susceptible protocol stacks across the network. The product is enterprise class, capable of assessing hundreds of thousands of hosts daily using dozens of scan engines controlled from a central point, all within the customer's firewall. Once assessed, a rich set of Vulnerability or Compliance reports may be generated in several formats, such as PDF, HTML, or XML, with full details on each detected vulnerability as well as steps to correct or remove the exposure or policy violation. A feature-rich remediation system is also available, with trouble ticket generation, ticket routing and historical tracking, e-mail notification, positive one-click verification, and optional automatic ticket closure.

In addition to proprietary Vulnerability and Compliance Scanning, McAfee Vulnerability Manager supports Benchmark Scans utilizing all six of the open SCAP standards: CVE, CPE, CCE, CVSS, XCCDF, and OVAL. By following these standards, scanning results can be used to monitor and audit compliance in accordance with government and private sector requirements. For example, SCAP data-feeds – such as the FDCC benchmarks for Windows XP, Windows Vista, and Internet Explorer 7 – can be directly imported to the product, as can custom content and community-developed security benchmarks. Both scans and reports can be scheduled or run ad-hoc across various grouping of assets or entire IP address ranges. Reports are human-readable, highly navigatable, and include standard XCCDF and OVAL XML results. Further, CPE values identify target platforms, CVE and CCE identifiers provide industry cross-reference to additional vulnerability and configuration-error information, and CVSS scores are used to rate system compliance.

McAfee Vulnerability Manager is compliant with SCAP Version 1.0.

Statement of FDCC Compliance

To remotely assess systems for Federal Desktop Core Configuration (FDCC) compliance using the McAfee Vulnerability Manager, certain FDCC constraints must be relaxed to allow for communication between a scan engine and each targeted computer:

- To assess Vista systems not connected to a domain, User Account Control (UAC) must be turned off on the target, thus enabling remote logons. This does not apply to Windows XP systems, nor to Vista systems joined to an Active Directory or Windows Networking Domain.
- Target systems of all types must have a firewall setting relaxed to allow remote file and registry access from each authorized scan engine. This should generally be scoped to one, or a small group, of specific IP addresses. Once past the firewall, actual connections between scanner and target are controlled via standard Windows Authentication and Authorization. The Remote Registry service must also be enabled at startup. Domain-wide Group Policy settings can easily be used to configure all these settings.
- The WMI service must be set to "Remote Enable" and a firewall rule relaxed to allow remote WMI access in order to properly read certain Password Policy settings, including "Password must meet complexity requirements" and "Store passwords using reversible encryption".

The preceding points apply specifically to scanning for FDCC compliance. Many other product features, including Unauthenticated Vulnerability Scanner, do not require relaxation of these rules. However, only open network-facing vulnerabilities will be reported in these cases.

McAfee Vulnerability Manager is compliant with FDCC Version 1.0.

Statement of CVE Implementation

With its world-renown Avert® Labs research team, McAfee has developed a broad database of proprietary vulnerability checks. When generating reports on the results of Vulnerability and Compliance Scans, pages are provided which name and document each detected out-point, including a description of the conditions causing the exposure or vulnerability and, where applicable and known, instructions for remediation. These report pages are generally available in several languages.

In contrast, the Common Vulnerabilities and Exposures (CVE) standard provides an open database which documents many publicly known computer security vulnerabilities and exposures. These are similar to the descriptions provided by Avert® Labs, but generally do not have remediation instructions. CVE entries typically contain a unique identifier, links to additional information, and a reference to the National Vulnerability Database (NVD) entry at http://nvd.nist.gov with a detailed description of the issue.

Many of the McAfee proprietary vulnerability checks used in Vulnerability and Compliance scans have a corresponding CVE identifier, while many are McAfee specific. When a check does have a corresponding CVE identifier, a direct link to the CVE details page at http://cve.mitre.org is provided in the report, supplementing the McAfee-supplied details already given. This linked-to page generally provides a further link into the National Vulnerability Database for additional information, as well as links to other references.

When running Benchmark Scans, such as when importing and evaluating SCAP content or other XCCDF benchmarks, the imported XCCDF and OVAL source files will often contain CVE links and other references. In those cases, McAfee Vulnerability Manager's Benchmark Scan reports will provide direct links to the official CVE details pages on the Internet, or to the other references, as specified in the imported content. The generated XCCDF and OVAL compliant XML output files will also contain these references.

McAfee Vulnerability Manager is compliant with CVE.

Statement of CCE Implementation

Common Configuration Enumeration (CCE) provides documentation for, and unique identification of, configuration issues – much in the same way that CVE (Common Vulnerability Enumeration) provides unique identifiers for common vulnerabilities and exposures.

When importing and evaluating SCAP content and other XCCDF benchmarks, the imported XCCDF and OVAL source files can contain CCE links and other references. In those cases, McAfee Vulnerability Manager's Benchmark Scan reports will provide direct links to the CCE details pages, or other references, as specified in the imported content. The generated XML output files, which are fully XCCDF and OVAL compliant, will also contain these references.

Further, while many of the proprietary checks developed by Avert® Labs at McAfee have to do with configuration issues, at the time of certification no direct mapping is being provided to CCE identifiers when running Vulnerability or Compliance Scans. This is subject to change based on public availability of content and customer demand.

McAfee Vulnerability Manager is compliant with CCE Version 4.0.

Statement of CPE Implementation

The Common Platform Enumeration (CPE) is a scheme for structuring computer software product, system, and platform identifiers as well as a dictionary which maps standard identifiers to corresponding human-readable product names.

Several McAfee products, including McAfee Vulnerability Manager, use a patented technique to fingerprint various protocol stacks and accurately determine the underlying platform, even without logging on to the target computer. These fingerprints are continually reviewed and updated to account for patches, updates, etc. so as to ensure the best possible accuracy. When combined with credentialed access to a target system, identification becomes even more accurate. These techniques identify many platforms covered by CPE, as well as many not presently named by CPE.

For Compliance and Vulnerability Scans, wherever a match exists the report will map the identified platform to a CPE value and display the associated CPE text.

For Benchmark Scans, when the imported XCCDF and/or OVAL content supplies a CPE identifier, that identifier will be reproduced in the XCCDF and OVAL compatible XML output, and the CPE human-readable text will be displayed on any associated reports. Further, CPE entries (via their associated OVAL definitions) can be used to restrict benchmark application to particular platform types.

McAfee Vulnerability Manager is compliant with CPE Version 2.0.

Statement of CVSS Implementation

The Common Vulnerability Scoring System (CVSS) is an open standard for identifying the severity of individual vulnerabilities or information exposures by reducing several visible factors (called "vectors") down to a single numeric score, which is comparable across products from different vendors.

For benchmark scans, if the imported XCCDF and OVAL content provides CVSS scoring information, then the resulting score will be calculated and displayed on benchmark reports for each system scanned and the vector made available in the supporting XML documents.

Anywhere that a CVSS score is displayed, a link to an off-line popup CVSS calculator is available, which allows tailoring the score for environmental and temporal concerns.

Many of the proprietary checks developed by Avert® Labs for McAfee include CVSS scores. Therefore, Vulnerability and Compliance Scan reports will often provide a CVSS score, as well as make available the underlying CVSS vectors, in the vulnerability details section. Such vulnerability and compliance scores include temporal modifiers that are updated regularly by McAfee Avert® Labs.

In addition, McAfee Vulnerability Manager provides a patented "network-wide risk score" called a FoundScore. This value provides an "at-a-glance" executive summary of the current security posture of an entire network or group of assets therein, given any particular Vulnerability or Compliance Scan. This value is quite useful for trending a network's overall security profile. Assets may be assigned criticality values used to weight the score for environmental concerns and each check includes a proprietary and constantly-maintained threat value used to weight for temporal concerns.

McAfee Vulnerability Manager is compliant with CVSS Version 2.0.

Statement of XCCDF Implementation

The eXtensible Configuration Checklist Description Format (XCCDF) is an open standard for describing security benchmarks and other types of checklists.

With close adherence to the XCCDF specification, McAfee Vulnerability Manager supports importing XCCDF documents which use OVAL checks for automated testing of information systems, scanning network assets for compliance with those benchmarks, then reporting on compliance in both human readable and machine readable forms (HTML and XML, respectively).

Once content is validated and imported, scans can be scheduled to periodically evaluate benchmarks against user-specified groups of assets, up to and including the entire customer network. Results are stored in a database, allowing for on-demand reporting across different scans utilizing the same benchmark.

By fully meeting SCAP document-input requirements, FDCC and other XCCDF benchmark files may be directly imported and used to monitor compliance of large networks of assets. McAfee Vulnerability Manager supports direct importation of entire SCAP data streams, in ZIP format, or importation of loose XCCDF, OVAL, and CPE dictionary XML files. In addition to customer supplied content, the product provides a rich set of built-in, professionally developed XCCDF and OVAL content, which can be used to help evaluate compliance with dozens of industry benchmarks including HIPAA, SOX, PCI-DSS, and many others.

By fully meeting SCAP document-output requirements, the XML results may be used to monitor and audit IT systems compliance in accordance with government and private sector requirements.

In addition to benchmark evaluation, McAfee Vulnerability Manager provides numerous industry templates for Vulnerability and Compliance Scans which use proprietary McAfee content. These are highly customizable and may be tailored to suit the needs of specific departments or individuals.

McAfee Vulnerability Manager is compliant with XCCDF Version 1.1.4.

Statement of OVAL Implementation

The Open Vulnerability Assessment Language (OVAL) is a public standard for creating vulnerability, configuration, and patch checks using a declarative XML syntax. Given logon-access to a target computer, it is suitable for examining a wide range of system attributes and either detecting or inferring the presence of configuration issues and vulnerabilities.

McAfee Vulnerability Manager supports an OVAL implementation conformant with the OVAL specification and is suitable for use with FDCC compliance scanning, reporting, and auditing.

OVAL checks are run in the context of an XCCDF Benchmark, producing OVAL and XCCDF compliant XML output as well as human readable HTML reports with rich hyperlinking to industry references and internal check details. This output fully meets SCAP requirements, allowing the results to be used to monitor and audit compliance in accordance with government and private sector requirements.

The product not only provides support for importing publically generated OVAL content, it also includes many OVAL checks developed for use with built-in XCCDF benchmarks, which help check compliance with dozens of industry standards including HIPAA, SOX, PCI-DSS, and more.

McAfee Vulnerability Manager further provides a huge database of checks written in a proprietary procedural language. These checks are suitable not only for examining machine state to detect vulnerabilities (configuration settings, file versions, registry values, file content, etc.), but in many cases checks can be (optionally) enabled which directly exercise protocol stacks across the network and intrusively prove the existence of vulnerabilities and exposures. Well over 15,000 professionally developed checks are provided, with more added weekly through dynamic product updates.

McAfee Vulnerability Manager is compliant with OVAL Version 5.5.